УДК 004.056:621.311.1

ВНЕДРЕНИЕ СИСТЕМЫ МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ДЕЯТЕЛЬНОСТЬ ПРЕДПРИЯТИЯ ЭНЕРГЕТИЧЕСКОЙ ОТРАСЛИ

С. Ю. Воробьёв, Е. А. Ханчевский

Научно-исследовательское и проектно-изыскательское республиканское унитарное предприятие «Белэнергосетьпроект»,
Минск, Беларусь, s.varabyou@besp.by, zh@besp.by

Цифровизация экономики ставит перед организациями энергетической отрасли задачи обеспечения надлежащего уровня информационной безопасности. В научной литературе отсутствуют исследования, посвященные внедрению системы менеджмента информационной безопасности в деятельность предприятий национальной энергетики. В статье описан процесс внедрения системы менеджмента информационной безопасности в деятельность предприятия, структурно входящего в состав ГПО «Белэнерго» Министерства энергетики Республики Беларусь.

Ключевые слова: энергетика; информационная безопасность; система менеджмента; СМИБ; ISO/IEC 27001.

IMPLEMENTATION OF AN INFORMATION SECURITY MANAGEMENT SYSTEM IN THE ACTIVITIES OF AN ENTERPRISE IN THE ENERGY INDUSTRY

S. Yu. Vorobyov, E. A. Khanchevsky

Scientific research and design and survey republican unitary enterprise "Belenergosetproekt", Minsk, Belarus, s.varabyou@besp.by, zh@besp.by

The digitalization of the economy poses challenges to energy industry organizations to ensure an appropriate level of information security. There are no studies in scientific literature devoted to the implementation of an information security management system in the activities of national energy enterprises. The article describes the process of implementing an information security management system in the activities of an enterprise that is structurally part of the GPO Belenergo of the Ministry of Energy of the Republic of Belarus.

Keywords: energy; information security; management system; ISMS; ISO/IEC 27001.

1. Введение

В белорусской энергетике наравне с другими отраслями национальной экономики происходят активные процессы цифровизации, что ставит перед организациями энергетической отрасли актуальные задачи по

обеспечению информационной безопасности (далее – ИБ) и защите информации (далее – ЗИ).

Вопросам ИБ на объектах энергетики посвящены работы белорусских и российских авторов С. Ю. Воробьёва, Е. А. Ханчевского, А. И. Белоуса, И. А. Костомахи, И. Н. Колоска, Е. С. Коркиной, М. Г. Головенчик, Г. Г. Краско, Г. Г. Головенчик, В. А. Северин, Д. Хитрых [1–7]. Эффективность внедрения системы менеджмента ИБ (далее – СМИБ) в деятельность предприятий и организаций проанализирована в статьях А. В. Вилковой, А. А. Кайсарова, А. Т. Касымбека, П. А. Лонцих, А. В. Суханова, М. Д. Хвистика, Л. А. Федоськиной, И. Ю. Шахалова [8–15].

Вместе с тем в настоящее время отсутствуют работы, посвященные исследованию эффективности от внедрения СМИБ в деятельность организаций энергетической отрасли.

Целью статьи является исследование проекта внедрения СМИБ в деятельность одного из предприятий, структурно входящего в ГПО «Белэнерго» Министерства энергетики Республики Беларусь (далее – Предприятие), анализ полученных от его реализации результатов, перспективы по дальнейшему укреплению состояния защищенности обрабатываемой информации в информационных систем (далее – ИС) Предприятия.

2. Основная часть

Набором общепризнанных международным сообществом требований и лучших практик, предъявляемых к СМИБ, является серия стандартов ISO/IEC 270xx, принятая Международной организацией по стандартизации ISO (International Organization for Standardization) [16]. После проведения мероприятий по переводу и терминологической адаптации Государственным комитетом по стандартизации Республики Беларусь данные технические нормативные правовые акты (далее – ТНПА) были введены в действие (по содержанию и смысловой нагрузке они полностью идентичны стандартам ISO). В национальной системе стандартизации действуют следующие из них:

– СТБ ISO/IEC 27000-2024 «Информационные технологии. Методы обеспечения безопасности. Общий обзор и словарь» – представляет собой обзор систем менеджмента информационной безопасности, которые являются предметом серии стандартов СМИБ, а также терминологическую базу связанных с ними терминов [17];

– СТБ ISO/IEC 27001-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования» (далее – СТБ 27001) – по сути является основным стандартом данной серии и

устанавливает требования к разработке, внедрению, поддержанию и постоянному улучшению СМИБ в контексте организации [18];

– СТБ ISO/IEC 27002-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью» (далее – СТБ 27002) предназначен для использования при разработке руководства по менеджменту ИБ в конкретных отраслях и организациях с учетом их специфики [19];

– СТБ ISO/IEC 27003-2014 «Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности» (далее – СТБ 27003) описывает процессный подход по определения и разработке СМИБ от начала до фактического завершения проекта [20];

– СТБ ISO/IEC 27004-2014 «Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения» представляет собой руководство по разработке и применению мер измерения и проведению процесса измерения внедренной СМИБ (в том числе средств управления или их совокупности) [21];

– СТБ ISO/IEC 27005-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по менеджменту рисков информационной безопасности» (далее – СТБ 27005), по авторскому мнению, является не менее значимым ТНПА, чем СТБ 27001, так как описывает механизм реализации выполнении требований, касающихся действий по рассмотрению рисков ИБ и менеджмента рисков ИБ [22].

Внедрение СМИБ в деятельность Предприятия имело под собой следующие основания:

– укрепление деловой репутации на рынке как высоконадежной организации, применяющей в своей деятельности наилучшие общепризнанные практики по информационной безопасности;

– получение лицензии для осуществления деятельности в сфере технической и криптографической защиты информации по проектированию, созданию и аудиту систем информационной безопасности критически важных объектов информатизации (в соответствии с ч. 4.3 ст. Закона Республики Беларусь от 14.10.2022 № 213-З «О лицензировании» (далее – Закон о лицензировании) необходимо наличие действующего сертификата соответствия Национальной системы подтверждения соответствия Республики Беларусь на систему менеджмента информационной безопасности [23]).

Реализация проекта по внедрению СМИБ осуществлялась согласно рекомендаций СТБ 27002 и СТБ 27003: были созданы рабочая группа и план внедрения СМИБ (с определением этапов, сроков реализации проекта и ответственных лиц). Состав рабочей группы подбирался исходя из требований СТБ 27001 к организации, в которой планируется внедрение

СМИБ: контекст (основной вид деятельности), соответствие нормативным и договорным требованиям в сфере ИБ, подбор и обучения персонала, проведение мероприятий по снижению рисков ИБ (что, как, правило требует существенных материальных затрат, например, на закупку антивирусного программного обеспечения или проведения мероприятий по сканирования сети). Таким образом в состав рабочей группы вошли руководители подразделений ИБ, информационных технологий, планово-экономического и бухгалтерии, правовой и кадровой работы. Возглавил рабочую группу первый заместитель директора – главный инженер, как непосредственный куратор основных производственных процессов Предприятия.

Рабочая группа начала свою деятельность с инвентаризации информационных активов Предприятия: информации, обрабатываемой в ИС и определения основных бизнес-процессов. Были подвергнуты ревизии локальные правовые акты (далее – ЛПА), регулирующие вопросы ИБ и ЗИ, на предмет их соответствия законодательным и нормативным требованиям. Результатом работы стали не только актуализация действующих локальных актов, но разработка новелл (например, предоставление возможности работнику работать дистанционно, в том числе с использованием собственного оборудования).

Необходимо обратить внимание, что СТБ 27001 не только не противоречит нормам национального законодательства, регулирующего вопросы ИБ и ЗИ, но прямо коррелирует с ним (согласно п. 5.31 Приложения СТБ 27001 правовые, законодательные, нормативные и договорные требования, относящиеся к информационной безопасности, и подход к выполнению этих требований в организациях должен быть идентифицирован, документирован и поддерживаться в актуальном состоянии).

При актуализации и разработке ЛПА в последние имплементировались требования правовых актов законодательства в данной сфере. Так, согласно Политике информационной безопасности роль представителя руководства Предприятия по вопросам информационной безопасности была возложена на первого заместителя директора – главного инженера, что коррелирует п. 3.15 Указа Президента Республики Беларусь от 14.02.2023 № 40 «О кибербезопасности» (далее – Указ № 40), в котором руководители организаций назначают одного из своих заместителей ответственным за организацию работ по кибербезопасности [24].

С целью повышения вовлечения всех работников Предприятия в реализацию проекта внедрения СМИБ и повышения осведомленности по вопросам ИБ и ЗИ проекты перерабатываемых ЛПА направлялись в структурные подразделения для ознакомления и получения обратной связи в виде замечаний и предложений (в случае наличия и актуальности последних в проекты ЛПА вносились соответствующие правки).

Была выявлена необходимость актуализации иных ЛПА Предприятия, непосредственно не входящих в документацию СМИБ: Положения о

коммерческой тайне, Политике о защите персональных данных, должностных инструкций некоторых работников.

Необходимо отметить, что ведомственные стандарты ГПО «Белэнерго» СТП 33243.01.216-16 «Подстанции электрические напряжением 35 кВ и выше. Нормы технологического проектирования» (далее – СТП 33243.01.216) [25] и СТП 33240.20.117-18 «Цифровые подстанции. Требования к проектированию» [26] в своей структуре содержат раздел, предъявляющий требования к ИБ при проектировании энергообъектов, и, соответственно, коррелируют с п. 5.8 Приложения А СТБ 27001, который предъявляет требования по интеграции ИБ в менеджмент проектов.

Внедрение СМИБ предъявляет требования к процессам, связанным с управлением людьми: подбору работников в соответствии с их профессиональными знаниями, умениями и навыками, надлежащими морально-этическими качествами, а также постоянному повышению осведомленности работающих в сфере ИБ и ЗИ. В соответствии со ст. 11 Декрета Президента Республики Беларусь от 15.12.2014 № 5 «Об усилении требований к руководящим кадрам и работникам организаций» стадия изучения кандидатов на вакантные должности Предприятия сопровождается запросами характеристики с предыдущего места работы и сведений из единого государственного банка данных о правонарушениях (в отношении кандидатов на руководящие должности) [27]. Требование о повышении квалификации работников подразделений ЗИ предусмотрены Указом № 40 (при этом работники центров кибербезопасности должны пройти обучение в республиканском унитарном предприятии «Национальный центр обмена трафиком» (далее – НЦОТ)) [24], Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» [28], приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449» [29]. Указом Президента Республики Беларусь от 28.20.2021 № 422 «О мерах по совершенствованию защиты персональных данных» владельцы критически важных объектов информатизации и собственники (владельцы) ИС, в которых обрабатывается информация, распространение и (или) предоставление которой носят ограниченный характер, обеспечивают не реже одного раза в три года обучение работников ИБ в Национальном центре защиты персональных данных (далее – НЦЗПД) [30]. В процессе внедрения СМИБ обучение на базе НЦЗПД и НЦОТ прошли не только специалисты по ИБ, но также руководители и работники иных структурных подразделений Предприятия.

Согласно парадигме обработки рисков ИБ, принятой СТБ 27005 и СТБ 34.101.70-2016 «Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах» [31], были проведены мероприятия по

идентификации уязвимостей активов Предприятия, выявлению потенциальных угроз, которые могут воздействовать на последние, оценке возможных последствий в стоимостном эквиваленте, и, соответственно, принятию мер по снижению рисков ИБ (в том числе были пересмотрены права предоставления доступа к ИС Предприятия, а также запланировано к приобретению и внедрению специализированное программное обеспечение: система предотвращения утечек конфиденциальной информации DLP (Data Loss Prevention).

Финальной стадией проекта согласно методологии, изложенной СТБ 27003, было проведение внутреннего аудита СМИБ на соответствие требованиям СТБ 27001. По результатам выявленных замечаний определены ответственные лица и сроки устранения.

На момент написания статьи Предприятием подана заявка на сертификацию СМИБ на соответствие требованиям СТБ 27001 в организацию, аккредитованную на проведение аудита и сертификации в Национальной системе аккредитации Республики Беларусь.

3. Заключение

Организации энергетической отрасли Республики Беларусь при осуществлении деятельности обрабатывают в ИС информацию, представляющую самостоятельный и ценный ресурс, нарушение конфиденциальности которой может привести к совокупности неблагоприятных последствий [32, с. 59]. Вызовом времени для энергетической отрасли является не только осознание необходимости в проведении комплекса мероприятий организационного, правового и технического характера по ЗИ, но и вовлеченность в последние работников всех уровней, в первую очередь, руководителей высшего звена.

Анализ описанного процесса внедрения СМИБ на Предприятии позволяет сделать следующие выводы.

1. Следование процессному подходу позволило определить цели внедрения СМИБ в деятельность Предприятия, заинтересованные стороны, участников проекта и сроки реализации.

2. В реализацию проекта был вовлечен весь персонал Предприятия: от директора до специалиста, что способствовало выделению необходимых материальных ресурсов в достаточном количестве, своевременной и качественной актуализации локальной правовой базы, внесению изменений и дополнений в должностные инструкции работников, повышению осведомленности последних по вопросам ИБ и ЗИ.

3. Предусмотренное Указами Президента Республики Беларусь [24, 28] повышение квалификации в сфере технической и криптографической ЗИ на базе НЦОТ и НЦЗПД прошли не только специалисты,

обеспечивающие ЗИ на Предприятии, но также ряд работников от заместителя директора до руководителей структурных подразделений.

4. На Предприятии ведется серьезная работа подбору и изучению кандидатов на вакантные должности, включая изучение моральных и деловых качеств, законопослушности и гражданской самосознательности.

5. СТБ 27001 коррелирует СТП 33240.20.117-18 и СТП 33243.01.216 в части менеджмента ИБ при реализации проектов.

6. Парадигма применения в СМИБ законодательных, нормативных и договорных требований позволяет гибко и адаптивно выстраивать локальную правовую базу, регулирующую вопросы ИБ и ЗИ, в том числе путем имплементации требований национального законодательства.

7. Реализацией проекта внедрения СМИБ процесс поддержания надлежащего уровня ИБ в организации не заканчивается (методологией СМИБ предусмотрены систематические мероприятия по переоценке рисков ИБ и проведения внутренних аудитов на соответствие требованиям СТБ 27001).

8. Подтверждение соответствия СМИБ требованиям СТБ 27001 в Национальной системе соответствия Республики Беларусь позволит Предприятию получить лицензию на право выполнения работ по проектированию, созданию и аудиту систем информационной критически важных объектов информатизации, а также укрепить деловую репутацию путем подтвержденного сертификатом декларирования следования нормативным требования ИБ.

СМИБ не является панацеей от хищения коммерческой тайны, обрабатываемой в ИС организации, или кибератаки на АЭС, но проведение мероприятий согласно методологии, основанной на рискориентированном подходе, описанной в стандарте СТБ 27001 позволит повысить защищенность самого ценного ресурса XXI века: информации.

Библиографические ссылки

1. *Воробьёв С. Ю., Ханчевский Е. А.* Кибератаки на критически важные объекты энергетики как источник угроз национальной безопасности // Энергетическая стратегия. 2024. Т. 102, № 6. С. 33–36.

2. *Белоус А. И.* Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения. Москва ; Вологда : Инфра-Инженерия, 2020.

3. *Костомаха И. А.* Методы удалённого проникновения злоумышленника в технологические сегменты сети предприятий электроэнергетики // Энергетик. 2024. № 8. С. 19–22.

4. *Колосок И. Н., Коркина Е. С.* Анализ кибербезопасности объектов энергетики с учётом механизма и кинетики нежелательных процессов // Энергетик. 2024. № 2. С. 3–8.

5. *Головенчик М. Г., Краско Г. Г., Головенчик Г. Г.* Проблемы кибербезопасности умных городов // Наука и инновации. 2020. № 12 (214). С. 51–57.

6. *Северин В. А.* Проблемы правового регулирования и методического обеспечения защиты информации в организациях ТЭК // Проблемы экономики и юридической практики. 2022. Т. 18, № 2. С. 96–103.

7. *Хитрых Д.* О цифровой трансформации энергетической отрасли // Энергетическая политика. 2021. № 10 (164). С. 76–89.

8. *Вилкова А. В., Литвишков В. М., Швырев Б. А.* Проблемы непрерывного обучения персонала информационной безопасности // Мир науки, культуры, образования. 2019. № 4(77). С. 29–31.

9. Внедрение международного стандарта ИСО/МЭК 27001 - основа управления информационной безопасностью предприятия / А. А. Кайсарова [и др.] // Вестник науки Южного Казахстана. 2018. № 4(4). С. 103–106.

10. *Касымбек А. Т.* Польза от внедрения международного стандарта ISO/IEC 27001 // Евразийское Научное Объединение. 2015. Т. 1, № 2(2). С. 52–53.

11. *Лонцих П. А., Сафонова О. М.* Методика создания и внедрение системы менеджмента информационной безопасности на промышленном предприятии // Системы. Методы. Технологии. 2020. № 4(48). С. 80–87.

12. *Суханов А. В., Смирнов А. С., Хитов С. Б.* Управление информационной безопасностью предприятий оборонно-промышленного комплекса в контексте стандарта ISO 27001:2013 // Научно-аналитический журнал «Вестник Санкт-Петербургского университета Государственной противопожарной службы МЧС России». 2017. № 1. С. 9–16.

13. *Хвистик М. Д., Серенков П. С.* Разработка и внедрение системы менеджмента информационной безопасности в соответствии с ISO/IEC 27001:2013 // Приборостроение-2021 : Материалы 14-й Международной научно-технической конференции, Минск, 17–19 ноября 2021 года / Минск : Белорусский национальный технический университет, 2021. С. 242–243.

14. *Федоськина Л. А., Рогачев Р. А.* Ключевые тренды в сертификации систем менеджмента информационной безопасности на основе международного стандарта ISO 27001 // Цифровая трансформация: тенденции и перспективы : Сборник трудов I Международной научно-практической конференции, Москва, 21 декабря 2022 года / Под ред. Н. Л. Кетоевой и М. Т. Заргарян. М. : Общество с ограниченной ответственностью «Издательство «Мир науки», 2022. – С. 199–207.

15. *Шахалов И. Ю., Райкова Н. О.* К вопросу об интегрировании систем менеджмента качества и информационной безопасности // Правовая информатика. 2014. № 2. С. 20–26.

16. ISO: the International Organization for Standardization. URL: https://www.iso.org/home.html (date of access: 17.07.2025).

17. Информационные технологии. Методы обеспечения безопасности. Общий обзор и словарь : СТБ ISO/IEC 27000-2024. (Введ. 25.10.2024) / Минск : БелГИСС, 2024.

18. Информационная безопасность, кибербезопасность и защита конфиденциальности. Требования : СТБ ISO/IEC 27001-2024. (Введ. 25.10.2024) / Минск : БелГИСС, 2024.

19. Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью : СТБ ISO/IEC 27002-2024. (Введ. 25.10.2024) / Минск : БелГИСС, 2024.

20. Информационные технологии. Методы обеспечения безопасности. Руководство по внедрению системы менеджмента информационной безопасности : СТБ ISO/IEC 27003-2014. (Введ. 14.08.2014) / Минск : Научн.-исслед. ин-т техн. защиты информации, 2014.

21. Информационные технологии. Методы обеспечения безопасности. Менеджмент информационной безопасности. Измерения : СТБ ISO/IEC 27004-2014. (Введ. 14.08.2014) / Минск : Научн.-исслед. ин-т техн. защиты информации, 2014.

22. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство по менеджменту рисков информационной безопасности : СТБ ISO/IEC 27005-2024. (Введ. 25.10.2024) / Минск : БелГИСС, 2024.

23. О лицензировании : Закон Респ. Беларусь от 14 октября 2022 г., № 213-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2025.

24. О киберобезопасности : Указ Президента Респ. Беларусь, 14 февр. 2023 г., № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2025.

25. Подстанции электрические напряжением 35 кВ и выше. Нормы технологического проектирования : СТП 33243.01.216-16. (Введ. 29.01.2016 ; с отменой на территории РБ СТП 09110.01.2.104-07) / Минск : Научн.-исслед. и проектно-изыск. респ. унитарн. предпр. техн. «Белэнергосетьпроект», 2016.

26. Цифровые подстанции. Требования к проектированию : СТП 33240.20.117-18. (Введ. 16.06.2018) / Минск : Научн.-исслед. и проектно-изыск. респ. унитарн. предпр. техн. «Белэнергосетьпроект», 2018.

27. Об усилении требований к руководящим кадрам и работникам организаций : Декр. Президента Респ. Беларусь, 15 дек. 2014 г., № 5 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2025.

28. О некоторых мерах по совершенствованию защиты информации : Указ Президента Респ. Беларусь, 16 апр. 2013 г., № 196 : в ред. Указа Президента Респ. Беларусь от 09.12.2019 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2025.

29. О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449. Республики Беларусь : Прик. Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2025.

30. О мерах по совершенствованию защиты персональных данных : Указ Президента Респ. Беларусь, 28 окт. 2021 г., № 422 : в ред. Указа Президента Респ. Беларусь от 24.03.2025 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. Минск, 2025.

31. Информационные технологии. Методы и средства безопасности. Методика оценки рисков информационной безопасности в информационных системах : СТБ 34.101.70-2016. (Введ. 12.08.2016) / Минск : Научн.-исслед. ин-т техн. защиты информации, 2016.

32. *Воробьёв С. Ю., Ханчевский Е. А.* Защита информации, представляющей коммерческую ценность, в организациях энергетической отрасли // Энергетическая стратегия. 2025. Т. 104, № 2. С. 59–62.